<table>
<thead>
<tr>
<th>Key</th>
<th>Algorithm Description</th>
<th>00/03</th>
<th>06</th>
<th>07</th>
<th>08</th>
<th>0A</th>
<th>0C</th>
<th>11</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIV Secure Messaging key (04)</td>
<td>3 Key Triple DES - ECB</td>
<td>×</td>
<td>×</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIV Authentication key (9A)</td>
<td>RSA 1024 bit modulus</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIV Card Application Administration key (9B)</td>
<td>RSA 2048 bit modulus</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital signature key (9C)</td>
<td>AES-128 - ECB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key management key (9D)</td>
<td>AES-192 - ECB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retired Key management keys (80-95)</td>
<td>AES-256 - ECB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card Authentication key (9E)</td>
<td>ECC: Curve P-256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetric</td>
<td>ECC: Curve P-384</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Mandatory and conditional data objects tested

- Card Capability Container
- Card Holder Unique Identifier
- X.509 Certificate for PIV Authentication
- X.509 Certificate for Card Authentication
- X.509 Certificate for Digital Signature
- X.509 Certificate for Key Management
- Cardholder Fingerprints
- Cardholder Facial Image
- Security Object

### Optional containers tested

- Printed Information
- Discovery Object
- Key History Object
- Retired X.509 Certificates for Key Management
- Cardholder Iris Images
- Secure Messaging Certificate Signer
- Secure Messaging Certificate Signer
- Pairing Code Reference Data Container

### Notes

- Use of Local PIN tested?
- Use of Global PIN tested?
- Local PIN Preferred tested?
- Global PIN Preferred tested?
- Use of OCC tested?
- VCI tested with pairing code?
- VCI tested without pairing code?